

Varonis

Varonis SaaS Data Security Platform

SOC 3

Service Auditor's Assurance Report

For the period

August 1, 2022 to July 31, 2023



Contents

Contents	2
Section I - Management Assertion Provided by Varonis	4
Section II – Independent Service Auditor’s Assurance Report Provided by KPMG	6
Varonis Management’s responsibilities	6
Service Auditor’s responsibilities	6
Framework Applied	7
Our Independence and Quality Control	7
Scope of work	7
Limitations of Controls at a Service Organization	7
Opinion	7
About this report including disclosure	8
Intended users and purpose	8
Section III - Description of Varonis SaaS Data Security Platform	10
Company Overview and Background	10
Description of the Services Provided	10
Infrastructure	10
System Boundaries	10
Separation of environments	11
Network Infrastructure	12
Security and Architecture	12
Data Center Security	12
Software	12
Physical Security	13
Access Control and User and Permissions Management	13
Quality Testing	13
Data	13
People	14
Change Management	14
Security Testing	14
Encryption	14
Human Resources processes	14
New Hire	14
Performance Evaluation	15

Whistleblower program _____	15
Organizational Structure _____	15
Authority and Responsibilities _____	15
Audit Committee _____	15
Communication _____	16
Risk Management _____	16
Enterprise Risk Management Program _____	16
Cyber Risk Assessments _____	16
Third-Party Risk Management _____	16
Privacy Management _____	16
Security and Privacy Awareness Training _____	16
Company Policies _____	17
Availability Procedures _____	17
Business Continuity Plan _____	17
Backup _____	17
Incident Response _____	18
Asset Management _____	18
Endpoint Security _____	18
Monitoring _____	18
Principal Service Commitment and System Requirements _____	18

Section I - Management Assertion Provided by Varonis

We have prepared the attached Description of Varonis SaaS Data Security Platform ('The System') for the August 1, 2022 to July 31, 2023 (the 'Description') based on the criteria in items (a)(i)–(ii) below, which are the criteria for a description of a service organization's system in paragraph 1.34 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Confidentiality and Privacy (the 'Description criteria'). The Description is intended to provide with information about the Varonis SaaS Data Security Platform system and managed moderation services system, particularly system controls intended to meet the criteria for the Security Principle set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy issued by the Assurance Services Executive Committee of the AICPA (applicable trust services criteria).

We confirm, to the best of our knowledge and belief, that:

- A. The Description fairly presents The System and managed moderation services controls system for the period August 1, 2022 to July 31, 2023 based on the following Description criteria:
 - i) The Description contains the following information:
 1. The types of services provided.
 2. The components of the system used to provide the services:
 - a) Infrastructure: the physical and hardware components of a system (facilities, equipment, and networks);
 - b) Software: the programs and operating software of a system (systems, applications, and utilities);
 - c) People: the personnel involved in the operation and use of a system (developers, operators, users, and managers);
 - d) Procedures: the automated and manual procedures involved in the operation of a system; and
 - e) Data: the information used and supported by a system (transaction streams, files, databases, and tables).
 3. The boundaries or aspects of the system covered by the Description;
 4. How the system captures and addresses significant events and conditions;
 5. The process used to prepare and deliver reports and other information to customers and other related parties;
 6. If information is provided to, or received from, subservice organizations or other parties; how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance and storage are subject to appropriate controls;
 7. For each principle being reported on, the applicable trust services criteria and the related controls that must be designed and operated effectively to meet those criteria, including as applicable:
 - a) Complementary user-entity controls contemplated in the design and operation of the service organization's system.
 8. For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria;
 9. Any applicable trust services criteria that are not addressed by a control and the reasons; and
 10. Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

- ii) The Description does not omit or distort information relevant to the service organization’s system while acknowledging that the Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.
- B. Subject to the information outlined in point c) below, the controls stated in the Description were suitably designed and operated effectively for the period August 1, 2022 to July 31, 2023, to meet the applicable trust services criteria. This assumes that the subservice organizations applied, for the specified period, the types of controls expected to be implemented and operated at the subservice organization and incorporated in the design of the system.

Varonis Inc

August 13, 2023



Section II – Independent Service Auditor’s Assurance Report Provided by KPMG

Private and confidential

The Board of Directors

Varonis

August 13, 2023

Dear Directors,

ISAE 3000 (SOC 2) Type II Independent Service Auditor’s Assurance Report.

In accordance with our engagement letter dated March 30, 2021, we have examined the accompanying Description at Section III of the controls in place at the service organization called Varonis ('The company') and carried out procedures to enable us to form an independent opinion on whether Varonis's management has fairly described Varonis SaaS Data Security Platform ('The System') and managed moderation services controls system throughout the specified period August 1, 2022 to July 31, 2023 (the 'Description'), and on the design and operation of controls stated in the Description to meet criteria for the Security, Confidentiality, Privacy and Availability Principle set forth in the TSP section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Technical Practice Aids) ('applicable trust services criteria'). Our opinion is set out below and should be read and considered in conjunction with this report in full.

Varonis Management’s responsibilities

In this report, references to Varonis's "management" means the directors of Varonis and those employees to whom the directors of Varonis have properly delegated day-to-day conduct over matters for which the directors of Varonis retain ultimate responsibility.

Management of Varonis is responsible for (1) preparing its statement at pages 8-9 and describing in the Description within the statement its system, including the completeness, accuracy and method of presentation of the same, (2) having a reasonable basis for its statement (3) selecting the criteria to be used and stating them in the statement, (4) specifying the controls that meet the applicable trust services criteria and stating them in the Description, and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the applicable trust services criteria will be achieved.

Service Auditor’s responsibilities

Our responsibility is to express an independent opinion to Varonis based on the procedures performed and evidence obtained, as to whether (1) Varonis's management Description fairly presents the controls system that was designed and implemented throughout the specified period and the aspects of the controls that may be relevant to a user organization's internal control, as it relates to an audit of the Security Principle within Varonis's statement, (2) the controls included in the Description were suitably designed throughout the specified period to provide reasonable assurance that the required trust services criteria would be met if the described controls



were complied with satisfactorily, and (3) such controls were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the required trust services criteria were achieved during the specified period.

Framework Applied

Our work was performed having regard to the framework set out by the International Auditing and Assurance Standards Board (IAASB) International Standard on Assurance Engagements International Standard on Assurance Engagements 3000 'Assurance Engagements Other than Audits or Reviews of Historical Financial Information' (ISAE 3000).

Our Independence and Quality Control

We comply with the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants. Accordingly, we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements and professional standards (including independence, and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior) as well as applicable legal and regulatory requirements.

Scope of work

An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's Description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description based on the Description criteria and the suitability of design and operating effectiveness of those controls to meet the applicable trust services criteria.

We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Limitations of Controls at a Service Organization

Varonis management's Description is prepared to meet the needs of their auditors. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in service operations or related reporting. Also, the projection of any evaluation of the effectiveness of the controls to meet the applicable trust services criteria to future periods is subject to the risk that the system may change or that controls at a service organization may become inadequate or fail.

The relative effectiveness and significance of specific controls at Varonis, and their effect on assessments of control risk at the user organization is dependent on their interaction with the controls and other factors present at the user organization. We have performed no procedures to evaluate the effectiveness of controls at the user organization.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects, based on the criteria identified in Varonis's statement on Section II and III and the applicable trust services criteria:



- A. The Description fairly presents The System and managed moderation services controls system that was designed and implemented throughout the period August 1, 2022 to July 31, 2023.
- B. The controls stated in the Description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the described controls were complied with satisfactorily throughout the period August 1, 2022 to July 31, 2023; and
- C. The controls tested, which were those necessary to provide reasonable assurance that the applicable trust services criteria were achieved, operated effectively throughout the period August 1, 2022 to July 31, 2023.

About this report including disclosure

This report is made to and has been prepared solely for the management of Varonis, as a body, on the terms agreed and recorded in our Engagement Letter. In this report, by “management” we mean the directors of Varonis and those employees to whom the directors of Varonis have properly delegated day-to-day conduct over matters for which the directors of Varonis retain ultimate responsibility.

This report was designed to meet the agreed requirements of Varonis and particular features of our engagement determined by Varonis’s needs at the time.

This report is confidential and is released on the basis that it shall not be copied, referred to or disclosed, in whole or in part, save as permitted by our Engagement Letter, without our prior written consent. We have consented to its disclosure to “User Entities”, being Varonis’s customer, the independent auditors of Varonis, practitioners providing services to Varonis and the prospective customers of Varonis. Our consent has been given without in any way or on any basis affecting our responsibility or giving rise to any duty or liability being accepted or assumed by or imposed on us to any party except Varonis and its management. We have consented to enable Varonis and its management to demonstrate, and such User Entities to verify, that an independent service auditor’s assurance report has been commissioned by the management of Varonis and issued in connection with the controls of Varonis.

Intended users and purpose

This report and Description of tests of controls and results on section IV are only to be disclosed to User Entities who have a sufficient understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization’s system interacts with user entities, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

The above understanding is necessary to enable the User Entities to consider the matters stated including the basis of our consent to disclosure and their ability to rely on this report, along with other information including information about controls implemented by customers themselves, when assessing the risks in relation to User Entities’ operational systems. This report is not to be used by anyone other than these specified parties.

This report does not restrict use by User Entities on the basis that those User Entities remain responsible for their own work and consideration of this report and for evaluating the evidence presented by our report and for determining its effect on the assessment of control risk at the User Entities.



SOMEKH CHAIKIN
KPMG Millennium Tower
17 Ha'arba'a Street
Tel Aviv, 6473917, Israel

TEL +972 3 684 8000
Fax +972 3 684 8444
Website www.kpmg.co.il

Any party other than Varonis or its management, as a body, who obtains access to this report or a copy and chooses to use and rely on this report (or any part of it) will therefore do so at its own risk. To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than Varonis and its management, as a body, for our work, for this report, or for the opinions we have formed.

Yours faithfully,



Somekh Chaikin

KPMG

Tel Aviv, Israel

August 13, 2023



Section III - Description of Varonis SaaS Data Security Platform

Company Overview and Background

Varonis started operations in 2005 and services numerous leading firms in the financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment, and education sectors.

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data, which includes sensitive files and emails, as well as confidential customer, patient, and employee data. Our services also protect financial records, strategic product plans, and other intellectual property from unauthorized access by nefarious actors.

The Varonis Data Security Platform detects cyberthreats from both internal and external actors by analyzing data, account activity, and user behavior, and thereby prevents and limits disaster by locking down sensitive and stale data, and efficiently sustains a secure state with automation.

Varonis products address additional important use cases including data protection, data governance, zero trust, compliance, data privacy, classification, and threat detection and response.

Description of the Services Provided

Varonis SaaS a cloud-hosted data security platform for protecting and governing enterprise data. Companies use Varonis SaaS to discover mission-critical data, ensure only the right people have access, and detect threats before they become breaches. Varonis integrates with a wide array of data repositories, applications, and infrastructure both on-premises and in the cloud to give customers a holistic view of their data. The Varonis Data Security Platform can be used to address these important use cases:

- **Detecting insider threats and cyberattacks** Varonis provides behavior-based threat detection that uses machine learning to alert on abnormal user or device behavior. Additionally, Varonis provides a live-updating library of pre-built threat models based on attack techniques and vulnerabilities used by real-world adversaries.
- **Pinpointing data exposure:** Varonis automatically classifies sensitive data, highlights where information is exposed externally or internally, and helps teams prioritize remediation efforts.
- **Limiting the blast radius of an attack:** Varonis safely automates permissions changes to eliminate unnecessary access and drastically reduce the damage from insider threats and cyberattacks.
- **Achieving compliance:** Varonis' vast library of classification rules can discover sensitive data related to GDPR, CCPA, HIPAA, and more. The permissions analysis and continual monitoring Varonis provides gives auditors a real-time pulse on compliance.

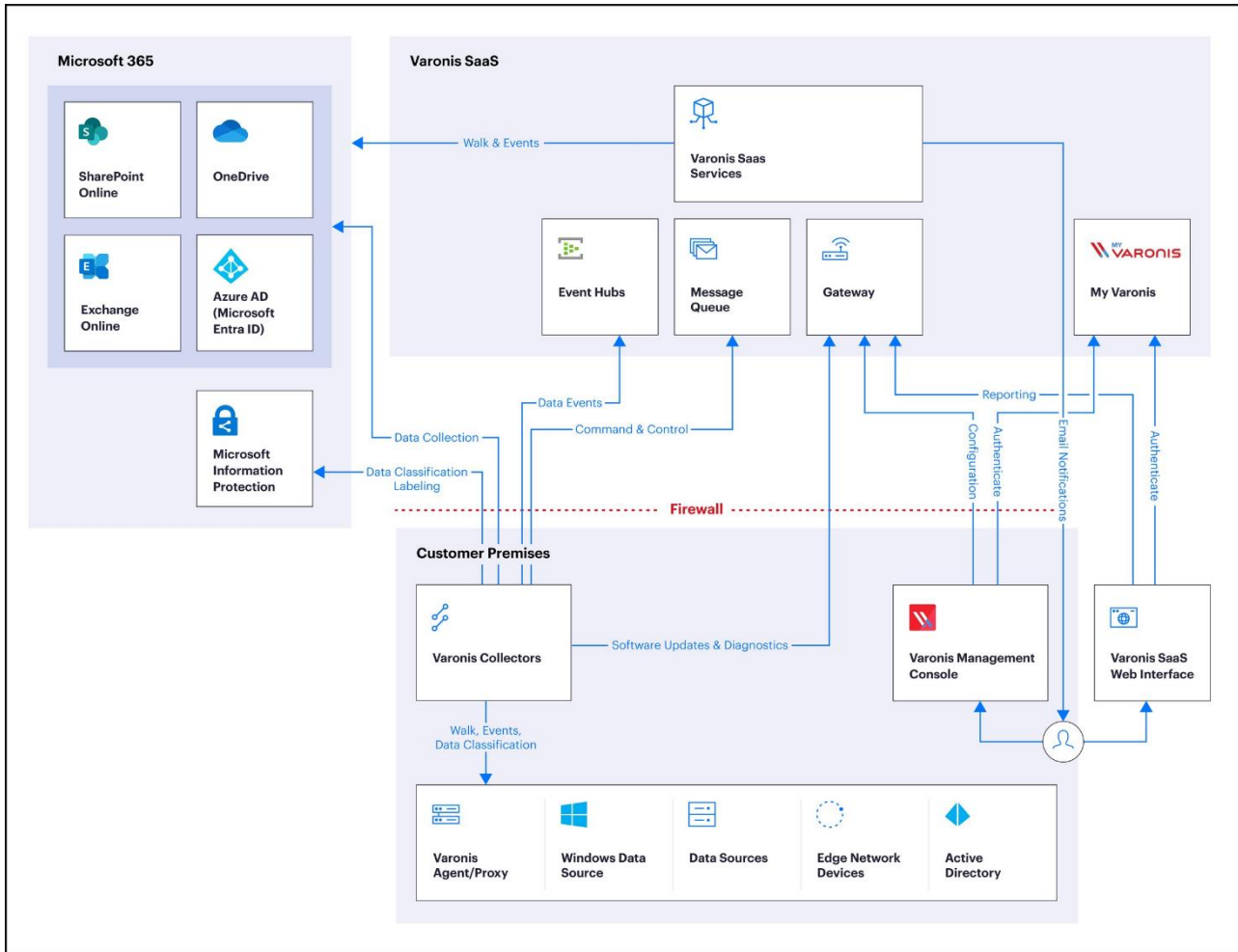
Infrastructure

Varonis' Software as a Service (SaaS) infrastructure is deployed on Microsoft Azure (utilizing both SaaS and Platform as a Service [PaaS] solutions) for hosting and operating production, staging, and development environments. Varonis leverages the experience, resilience, and reliability of Azure to scale quickly and securely to meet the current and future demands of its customers.

Each boundary of the system has specific security controls. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system.

System Boundaries

Varonis' SaaS infrastructure is implemented in Microsoft Azure and uses Okta as the identity provider for customer access and service level agreement authentication. The Varonis solution leverages the capabilities, resilience, and reliability of Microsoft Azure to scale quickly and securely to meet our customers' current and future demands.



Varonis monitors various platforms such as NetApp and Windows as seen in the diagram above. A Varonis Collector server installed on-premises is responsible for

- Monitoring those platforms gathering events and telemetries
- Collecting and auditing user activity events and file server metadata
- Classifying file contents using rule packs that Varonis provides
- Securely sending data to the cloud for analysis and processing
- Publishing DataAlert alerts

Varonis' Deployment Hub is responsible for all on-premises deployment flows. Varonis' SaaS user interface comprises the following applications:

- Varonis Management Console - for environment configuration
- Varonis Web Interface - for query and data analysis

Secured ports are used for both the Varonis Collector and the Deployment Hub when transferring data internally and externally.

Separation of environments

The production environment is separated from the staging and development environments with separate access control and segmented network.



Network Infrastructure

Robust network infrastructure is essential for reliable and secure real-time data communication between Varonis cloud service components. To provide sufficient capacity, Varonis' network infrastructure relies on platforms provided by Microsoft Azure and other software providers. To ensure appropriate network security levels, security standards and practices are backed by a multi-layered approach aimed at preventing security breaches and ensuring confidentiality and availability.

Security and Architecture

Varonis provides a secure, reliable, and resilient SaaS platform that has been designed from the ground up based on industry best practices. All secrets, such as tokens for connecting to customer databases, are stored in the Microsoft Azure key vault. Varonis uses Azure-managed identities to perform periodic security principal password rotation. Varonis has multiple security zones to differentiate services of various sensitivities and different service principles to isolate secrets. The keys that are under Varonis' responsibility (e.g., the password for tenant databases) are periodically rotated.

The sections below describe the network and hardware infrastructure, software, and information security elements that Varonis delivers as part of the platform, database management system security, and application controls.

Data Center Security

Varonis relies on Microsoft Azure's global infrastructure, including the facilities, network, hardware, and operational software, all of which support the provisioning and use of basic computing resources and storage. These facilities comply with industry standards of security and reliability, thereby enabling Varonis to provide its services in an efficient and stable manner.

Software

The Varonis application includes the following primary service components:

- Virtual machines, Service Fabric, and batch for online and batch processing
- Message broker
- Logging and monitoring
- Firewall and web application firewall
- Change management
- Blob storage service
- Key management system
- Identity and security management
- Programmable communication application program interfaces (APIs) for messaging
- Database applications
- Simple Mail Transfer Protocol (SMTP) provider
- Security information and event management
- Certificate management solution
- Managing observability platform
- Domain Name System (DNS) service

- Event hubs
- Structured Query Language (SQL) Server

Physical Security

Varonis maintains a physical security policy that aligns with industry best practices. The policy details procedures for securing offices globally, access restrictions to buildings and offices, badge access, periodic review of entry, and continuous workplace monitoring.

Our partner data center, Microsoft Azure, is SOC 2 compliant. The SOC 2 report addresses various physical security and environmental controls that are tested annually, and the Varonis security team reviews certificates and attestation reports annually to ensure a consistent level of protection.

Access Control and User and Permissions Management

Varonis' users are provided with the minimal access rights required to carry out their duties (known as "least privilege" access). Employees are assigned to a specific group upon hire. Employees who are assigned to the production group can request access to production. Their access is reviewed periodically by the business owners. When a user from that group requests access to production, the request must be approved by the business owner for each session. Access is limited by time and then documented, logged, and monitored by the security operations center. Employees accessing Varonis SaaS Platform and the corporate network are required to use a two-factor authentication mechanism and a virtual private network (VPN). Logical and physical access is revoked from resigned employees upon termination.

Customer access is authenticated in the system either by logging in with an applicable user-assigned ID or federated by the customer or through the customer's identity provider, which is supported by the system.

Quality Testing

Varonis' Validation and Quality Assurance (QA) team is involved from the early stages of development. Automatic tests are performed using a dedicated tool to validate the code quality. Code review is mandatory to continue the Secure Software Development Lifecycle (SSDLC) process. Successful test status is mandatory to continue in the SSDLC process and deploy a version to the production environment.

Data

Varonis differentiates between data and metadata:

1. Customer metadata includes user IDs and names, group names, folder and file names, email subjects, domains, and IP addresses that user's access.
2. Customer data includes both file and email contents. All customer metadata is classified as "confidential" per the Varonis Global Classification Policy. Customer data is securely stored and monitored to identify immediate or potential risks within the customer's environment.

Varonis technology crawls data sources, classifying customer data. Customer data is then retrieved and processed by the Collector servers installed inside the customer network only. Varonis SaaS Data Security Platform does not store customer data in the cloud*.

Metadata and data classifications are uploaded into SaaS for further customer use. The data is gathered and stored in protected storage for further analysis and to identify immediate or potential risks in the customer's environment. This information, including any alerts that are produced, is easily viewed on the Varonis SaaS dashboard. All customer metadata is always stored and transferred in encrypted form.

*Customers could enable the optional "File Analysis" role in the cloud, which allows customer users with an approved File Analysis role to retrieve specific files via SaaS. without storing them.



People

The Varonis employees involved in the development, operation, security, or support of the Varonis SaaS platform are grouped in the following primary areas:

- Executive Management
- Product Management
- Product Security
- Software Engineers
- DevOps
- Information Security
- Human Resources
- Professional Services
- Support
- Internal Audit
- Legal

Change Management

All changes to Varonis' services follow a structured process to ensure appropriate planning and execution. This structured process requires communication, documentation of important process workflows and personnel roles, and the alignment of automation tools where appropriate.

Software changes are tested in the development environment, committed to a source code management system, and reviewed through automated testing or by peers. Releases are tested by QA before deployment.

Varonis assigns customers to different "rings" so that software and configuration changes are gradually phased into production, one ring at a time; there is a delay between each ring release, thus minimizing impact in case of incorrect changes.

Security Testing

Various sets of security testing are performed on the cloud infrastructure and applications. Testing includes, but is not limited to, penetration testing that is performed by both an internal red team and on an annual basis by a reputable third-party vendor, vulnerability scanning, software composition scanning, code reviews, and other automated scans.

Encryption

Varonis uses Transport Level Security (TLS) to encrypt and provide integrity to all data when transmitting data over public networks. Encryption is for data at rest stored on virtual machines, databases, data backups and all other storage types. Communication between the boundaries is encrypted.

Human Resources processes

Hew Hire

Individuals offered a position at Varonis are subject to background checks (as appropriate for each country and considering local laws and regulations) as a condition to their employment in the company. In each location, employees receive data packages containing an overview of Varonis' Human Resources policies and procedures. These packages include the offer letter or employment contract, NDA, and the Varonis Code of Conduct. Employees are asked to sign their offer/employment



contract to confirm that they have read these materials and agree to be bound by their terms. New hires are also required to sign a privacy addendum. If background checks are not permitted in their country of employment, they undergo a reliability test.

Performance Evaluation

Varonis has a continuous performance management process that provides feedback to employees and managers through regular 1:1 meetings and Goal Plans in HR. Varonis also has an annual performance review process in place to review accomplishments, provide constructive feedback, identify opportunities for improvement, and ensure the ongoing development of all Varonis employees. The annual performance reviews enable managers to provide ratings for the direct reports on their team, employees to provide self-evaluations, and end with a year-end conversation between the managers and employees. This process is designed to align the employee's efforts and the organization's goals.

Whistleblower program

Varonis has an anonymous whistleblower program in place for employees to report any violation without fear of dismissal or retaliation. Reported issues are investigated and acted on in a timely manner. Information regarding how to report any violation is outlined in Varonis' Code of Business Conduct and Ethics policy.

Organizational Structure

Varonis has an established organizational structure with defined roles and responsibilities that are segregated based on functional requirements. The organization chart delineates lines of reporting and is updated in real-time to reflect any changes.

Authority and Responsibilities

Lines of authority and responsibility are clearly established throughout the company. Varonis' Board of Directors meets periodically to review committee charters and corporate governance that define their roles, responsibilities, member qualifications, meeting frequency, and other discussion topics. Minutes of the annual meetings are recorded and include the names of the participants and the date the meeting occurred.

The Board of Directors and management recognize their responsibility to foster a strong ethical environment within Varonis to determine that its business affairs are conducted with integrity and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Varonis Code of Business Conduct and Ethics, which is distributed to all employees. Specifically, employees and their immediate families are prohibited from using their positions at Varonis for personal or private gain, disclosing confidential information regarding customers or taking any action that is not in the best interest of the customers. Employees' personal securities transactions are governed by a corporate policy and employee account trades are reviewed to monitor adherence to Varonis' policy. All employees are required to maintain ongoing compliance with all policies, standards, and procedures of the Code of Conduct and with lawful and ethical business practices, whether they are specifically mentioned in the Code of Conduct or not. All employees are required to affirm annually that they received, read, understand, and comply with the requirements set forth in the Code of Conduct and the Employee Handbook. Employee recertification status is monitored periodically for compliance.

Audit Committee

The Audit Committee is responsible for overseeing and monitoring the integrity of Varonis' consolidated financial statements, the company's compliance with legal and regulatory requirements as they relate to financial reporting or accounting matters, and the company's internal accounting and financial controls. The Audit Committee also oversees and monitors Varonis' independent auditor's qualifications, independence, and performance; provides the Board of Directors with the results of its monitoring and recommendations; provides the Board of Directors with the additional information and materials it deems necessary to ensure the Board of Directors is aware of significant financial matters that require the Board's attention; and oversees Varonis' internal audit function.



Communication

Varonis values transparent communication—both internally and externally. Varonis communicates with prospects, customers, and employees through several methods including, without limitation, the corporate website, which includes our privacy policy and public ways to report product flaws or security issues, a customer portal, which contains product release notes and other critical product information, and an internal employee portal which offers information about policies and procedures.

Varonis' security approach and compliance certifications are documented and communicated to customers on Trust & Security, in the company's agreements, and as part of the description of services provided online.

Risk Management

Varonis has developed a risk management policy that includes risk identification, analysis, communication and reporting, treatment, and monitoring. The risk management program implements a structured security plan. Each risk is evaluated by the likelihood and impact it may cause, and the treatment plan is an ongoing effort by all Varonis departments.

Enterprise Risk Management Program

The security and privacy risk management program has several levels and is conducted periodically by external and internal auditors. High-level risks are covered during the annual enterprise risk assessment performed by the internal auditor and are presented to the company's senior management. The Chief Information Security Officer (CISO) conveys cyber threats, and a mitigation plan is then decided upon and implemented.

Cyber Risk Assessments

Varonis performs routine technical risk assessments for software development, cloud production, and corporate and cloud infrastructure (see security testing for more information). Expert third-party consultants also perform ongoing assessments. The Information Security Department, led by the CISO, monitors the progress of such efforts until all substantial risks are remediated. The CISO and senior management propose remediation plans, and the security steering committees decide on the treatment plan to be adopted.

Third-Party Risk Management

Engagements with third-party suppliers undergo a security risk assessment. It is incumbent upon Varonis to ensure that vendors are capable of delivery and aware of inherent security risks. The vendor is thoroughly vetted for security and posture. We assure our customers that their data is protected and evaluate the risk by thoroughly reviewing third parties' security, compliance, and privacy practices. Whenever customer data is shared with a new third party, our customers are notified, and the vendor list is updated. High-risk third parties that hold customer data undergo periodic reviews. Each engagement with potential disclosure of PII requires a privacy assessment and signing of a Data Processing Addendum. We also require a Non-Disclosure Agreement (NDA) and security agreements.

Privacy Management

Varonis is committed to complying with all applicable data protection laws and regulations and maintaining appropriate procedures and work instructions as part of its privacy information management system. The privacy program is aligned with global privacy standards, including the EU's GDPR.

Varonis implements a Privacy by Design strategy which limits the scope and scale of data collection and processing only to the minimum extend required, to limit risks to sensitive data. All personally identifiable information (PII) is collected and maintained for specifically stated purposes only.

Varonis is committed to upholding contractual terms related to privacy and data protection in its agreements with its partners, subcontractors, and other relevant third parties (customers, suppliers, etc.). Varonis has a designated Data Protection Officer who guides Varonis on all data privacy concerns, risk management, and other related legal matters.

Security and Privacy Awareness Training

Varonis' employees undergo information security and privacy awareness training upon joining the company, as well as

annually thereafter, in conformance with the information security policy. The training ensures that each group of employees receives security training according to their technical knowledge and needs.

Company Policies

- Acceptable use of assets
- Access control
- Asset management
- Backup and restore
- Business continuity
- Change management
- Cloud security
- Compliance
- Cryptography
- Data classification
- Data disposal
- Endpoint security
- Human Resources security
- Incident response
- Information security awareness, education, and training
- Information transfer
- Logging and monitoring
- Mobile device management
- Network security
- Passwords
- Physical and environmental security
- Privacy management
- Records retention and data disposal
- Risk management
- Secure software development lifecycle
- Supplier relationships
- Teleworking and remote access
- Threat and vulnerability management

Availability Procedures

High availability eliminates single points of failure to ensure continuous operations and extended uptime. Load balancing is used to distribute traffic across multiple servers. High availability and load balanced arrays are in place for production systems to help mitigate the effect of a system error. Additionally, Varonis implemented a web application firewall to protect against denial-of-service attacks and reduce the risk of web application threats.

Business Continuity Plan

Varonis' Business Continuity Plan outlines measures to avoid disruptions to customers and partners. The plan includes impact analysis and risk assessment to help identify critical functions and processes. Customer support and resiliency are top priorities. The plan includes a strategic continuity plan for customer support, including systems, suppliers, and users. The Business Continuity Plan also includes the following topics:

- Corporate infrastructure
- Critical suppliers
- Cyber incident response
- Pandemic preparedness

Backup

The database and storage are hosted on Microsoft Azure. A daily backup is performed using an automated application. In case of failure, a notification is sent to the operations team. Production databases utilize Azure availability zone capabilities. Additionally, a complete replica is stored at a separate region.



Incident Response

Varonis has implemented incident response policies and procedures to detect, investigate, and respond to security incidents. These procedures guide Varonis personnel in reporting and responding to information technology incidents that affect the security, availability, and confidentiality of the system. The Incident Response plan contains procedures to address various cybersecurity scenarios that may occur. Furthermore, the plan includes roles and responsibilities, and the communication process for stakeholders at each phase.

Asset Management

Company assets are tracked and managed throughout the asset lifecycle. Each asset has an owner assigned to it, to ensure there is an individual responsible for securing the asset. The tracked assets include production components as well as employee devices that may contain personal data. When assets reach end of life, they are securely destroyed to ensure that data is not recoverable.

Endpoint Security

Devices issued to company personnel must meet minimum security criteria, including full disk encryption, screen lockout policy, running antimalware and other security software, and being kept up to date with security patches.

Monitoring

Varonis uses a set of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders by an internal communication tool based on predefined rules and are then reviewed and processed according to their level of urgency.

Principal Service Commitment and System Requirements

Varonis' commitments to customers include security, confidentiality, availability, and privacy. Commitments are communicated and documented within agreements, the Trust & Security page, and as part of the supplier relationship process. Our commitments to our customers include, but are not limited to:

- An established global risk management process to identify, monitor, and manage risks for the entire organization, business units, and all supplier relationships.
- Controlled physical, logical, and remote access to sensitive information to reduce the likelihood of a security incident. Varonis has established and follows specific access control practices to protect information and information systems from unauthorized access, modification, disclosure, or destruction.
- Secure data transmission protocols to encrypt data in transmission over public networks. Encryption is also enabled on databases, data at rest, data backups, and communication between segmented boundaries.
- Network segregation to enforce separation between production, staging, testing, and other cloud-based and internal infrastructure environments.
- Minimum standards of security for the development, provision, and use of Varonis cloud services require that the security, confidentiality, availability, and privacy of assets within Varonis cloud services are protected. Risks to the services and to customers are subject to a risk assessment and to the application of suitable technical and organizational controls.
- Data centers that host, store, and/or process customer production data must comply with industry best practices. This includes protecting information system equipment and cabling, entrance controlled by access card, surveillance cameras, providing emergency power, shutoff, lighting, fire alarms, protection from water and fire, and maintaining temperature and humidity controls.
- A retention policy that complies with applicable legal, regulatory, and contractual requirements. This includes deleting customer data upon request or automatically based on lifecycle policies that are communicated to the customer.

- The Human Resources department (HR) ensures successful operations and delivery of effective security controls. This includes implementing security measures prior to employment, during employment, at termination, and as otherwise required during any other changes in employment status, as well as providing ongoing cybersecurity awareness training to the company's employees.
- Backup procedures designed to ensure the continued availability and accessibility of information and to minimize the cost of a disruption (e.g., operational error, disaster, or sabotage that causes damage to, or destruction of, information).
- Maintaining a service level agreement (SLA) between Varonis and its customers wherein Varonis' responsibilities and the customer's cooperation requirements are specified. Within such SLA, Varonis upholds certain obligations regarding the availability of its service, and maintaining support levels, depending on the severity of the error.
- Implementing privacy by design within the systems and processes, which is intended to minimize risks to privacy rights and to process personally identifiable information (PII), in keeping with regulatory requirements.